AUTHENTICATION METHODS AND TECHNIQUES: A REVIEW

Annu Khurana[1], Neeraj Jain[2]
[1]M.Tech Scholar, [2]Associate Professor
[1,2]Department of Electronics & Communication Engineering,
Modern Institute of Technology & Research Centre, Alwar (Raj),India.

Abstract: In the previous couple of years, we've seen that even the greatest organizations are not invulnerable to security ruptures. Top brasses like LinkedIn, Target, Home Depot and Sony Pictures have had their frameworks hacked into, uncovering touchy data of their proprietors, representatives, asnd customers. With a huge number of passwords, email locations and all the more having been uncovered, there has been a press the individuals who handle undertaking security to up their safeguards. This paper reviews on the authentication methods and concepts involved in it.

Keywords : User Authentication,Biometeric

I. INTRODUCTION

Authentication is the way toward confirming the personality of an individual or computerized element. It is a major part of data security that basically approves that substances are who or what they guarantee to be. It is regular for authentication to utilize physical attributes, for example, fingerprints, mystery information, for example, passwords and security instruments, for example, shrewd cards. [1]

Authentication is the way toward deciding if a person or thing is, truth be told, who or what it pronounces itself to be. Authentication innovation gives access control to frameworks by verifying whether a user's accreditations coordinate the certifications in a database of approved users or in an information authentication server. Users are normally related to a user ID, and authentication is cultivated when the user gives an accreditation, for instance a secret word, that matches with that user ID. Most users are most acquainted with utilizing a secret word, which, as a snippet of data that ought to be known uniquely to the user, is known as an information authentication factor. Other authentication variables, and how they are utilized for two-factor or multifaceted authentication (MFA), are portrayed underneath.

Authentication is significant on the grounds that it empowers associations to keep their systems secure by allowing just validated users (or procedures) to get to its ensured assets, which may incorporate PC frameworks, systems, databases, sites and other system based applications or administrations. When confirmed, a user or procedure is normally exposed to an approval procedure too, to decide if the verified substance ought to be allowed access to an ensured asset or framework. A user can be confirmed yet neglect to be offered access to an asset if that user was not conceded consent to get to it. [1]

The terms authentication and approval are regularly utilized reciprocally; while they may frequently be executed together the two capacities are particular. While authentication is the way toward approving the personality of an enlisted user previously enabling access to the secured asset, approval is the way toward approving that the confirmed user has been allowed authorization to get to the mentioned assets. The procedure by which access to those assets is limited to a specific number of users is called access control. The authentication procedure consistently precedes the approval procedure. User authentication happens inside most human-to-PC connections outside of visitor accounts, consequently signed in records and booth PC frameworks. By and large, a user needs to pick a username or user ID and give a substantial secret word to start utilizing a framework. User authentication approves human-to-machine collaborations in working frameworks and applications, just as both wired and remote systems to empower access to organized and web associated frameworks, applications and assets. [2]

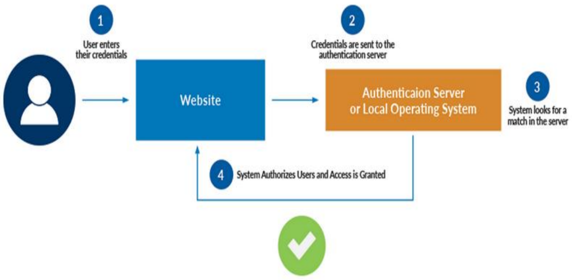
1
User enters their credentials
2
Credentials are sent to the authentication server
Website
Authenticaion Server or Local Operating System
3
System looks for a match in the server
4
System Authorizes Users and Access is Granted

Fig 1. Authentication Concept

Numerous organizations use authentication to approve users who sign into their sites. Without the correct safety efforts, user information, for example, credit and charge card numbers, just as Social Security numbers, could get under the control of cybercriminals. Associations likewise use authentication to control which users approach corporate systems and assets, just as to distinguish and control which machines and servers approach. Organizations additionally utilize authentication to empower remote workers to safely get to their applications and systems.[2]

For ventures and other huge associations, authentication might be cultivated utilizing a solitary sign-on (SSO) framework, which awards access to various frameworks with a solitary arrangement of login qualifications. During authentication, accreditations given by the user are contrasted with those on record in a database of approved users' data either on the nearby working framework or through an authentication server. On the off chance that the accreditations coordinate, and the validated element is approved to utilize the asset, the procedure is finished and the user is conceded get to. The authorizations and envelopes returned characterize both the condition the user sees and the manner in which he can communicate with it, including long periods of access and different rights, for example, the measure of asset extra room[3].

II. AUTHENTICATION METHODS

Biometrics for Network Security

The expression "biometrics" actually means the expression "estimating life". Biometrics additionally alludes to utilizing the known and archived physical ascribes of a user to confirm their character. This is perfect since no two individuals share precisely the same physical attributes. Basic biometric authentication strategies incorporate unique mark distinguishing proof, voice acknowledgment, retinal and iris outputs and face examining and acknowledgment. The drawback to this strategy is that it requires particular checking gear, which isn't perfect for certain businesses. [4]

Fig 2. Biometeric Security

Token Authentication

A token is a material gadget that is utilized to access secure frameworks. Basic structures incorporate a dongle, card or RFID chip. A token makes it increasingly hard for a programmer to get to a record since they should have long accreditations and the unmistakable gadget itself, which is a lot harder for a programmer to get.

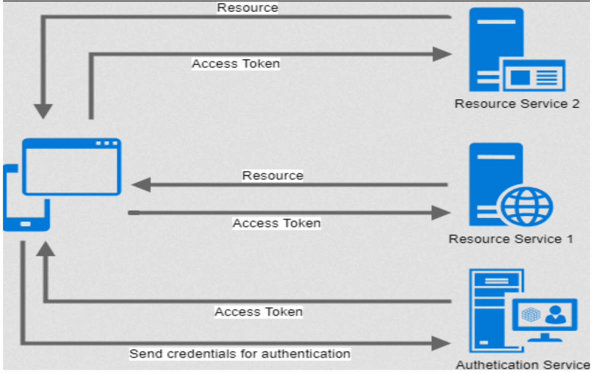

Fig 3. Token Authentication

Transaction Authentication

Transaction authentication searches out sensible mix-ups when contrasting known information about a user and the subtleties of an ebb and flow transaction. A model would be if an individual lives in the United States, yet enormous buys appear while signed in from an IP address abroad. A warning is sent up, and this reason for concern requires more check ventures to guarantee that the buy is real and that the user isn't a casualty of a digital wrongdoing.

Multi-Factor Authentication (MFA)

MFA is an authentication plan that requires at least two autonomous methods for confirming a character. Models incorporate something that the user has, for example, a phone or other physical token, inborn factors like biometric characteristics or something known like a secret key. ATM's are prime instances of MFAs since you need a card (physical token) and a PIN (something known) all together for the transaction to occur. [5]

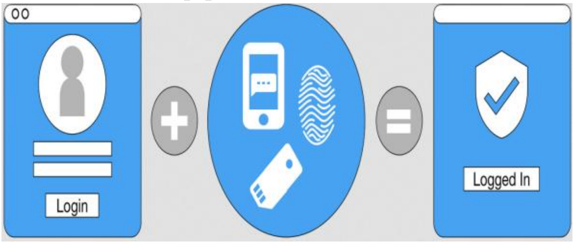

Fig 4. Multi-Factor Authentication

Out-of-Band Authentication (OOB)

OOB uses absolutely separate channels, similar to cell phones, to confirm transactions that started on a PC. Any transaction that requires stores starting with one spot then onto the next, similar to an enormous cash move, would produce a telephone call, content or warning on an application that there is more authentication required for the transaction to be finished. With two fundamental channels, it is significantly more hard for a programmer to take cash.[5]

Peripheral device recognition

Utilizing peripheral device recognition as a subsequent factor is cultivated by putting a cryptographic device marker on a user's current device, for example, a USB blaze drive, an iPod, Smart Phone memory card and after that necessitating that device to be connected to the PC when the user signs into the web based financial Web webpage. This can be great option in contrast to the OTP token since it gives an equipment based second factor however doesn't require the user to convey an extra device. Also, device markers from multiple banks can live on a solitary equipment device without requiring the different banks to incorporate their frameworks[5].

Scratch-off card

Utilizing a Scratch-off card as a subsequent factor is cultivated by issuing the user a card containing a few PIN numbers that the user scratches off and afterward utilized just one an opportunity to sign in. This is a lower-cost, once secret phrase choice than tokens. Note that TriCipher truly loves the "PC recognition software" strategy - the one I like least, in an online transaction condition, that is. I utilize a wide range of PC stages to collaborate with organizations on the web, organizations where I have accounts and burn through cash (or set aside cash, if it's the bank). I travel a great deal yet at the same time need to burn through cash, pay charges, check adjusts, and so on. Any solid authentication technique attached to one explicit PC really hampers my entrance while not so much giving an accompanying increment in security. I do like biometrics, yet I truly like utilizing my mobile phone for out-of-band check. Either through voice or SMS, it's the framework I wish more people would embrace[6]

III. COMMON ATTACKS ON SECURITY

Password attack

Since passwords are the most generally utilized component to confirm users to a data framework, getting passwords is a typical and powerful attack approach. Access to an individual's password can be gotten by checking out the individual's work area, "sniffing" the association with the system to obtain decoded passwords, utilizing social designing, accessing a password database or outright speculating. The last methodology should be possible in either a random or methodical way:

Brute-force password speculating means utilizing a random methodology by attempting various passwords and trusting that one work Some rationale can be connected by attempting passwords identified with the individual's name, work title, side interests or comparable things. In a lexicon attack, a word reference of normal passwords is utilized to endeavor to access a user's PC and system. One methodology is to duplicate an encoded document that contains the passwords, apply a similar encryption to a word reference of regularly utilized passwords, and analyze the outcomes.

SQL injection attack

SQL injection has turned into a typical issue with database-driven websites. It happens when a malefactor executes a SQL inquiry to the database by means of the information from the customer to server. SQL commands are embedded into information plane contribution (for instance, rather than the login or password) so as to run predefined SQL commands. An effective SQL injection endeavor can peruse touchy information from the database, adjust (addition, update or erase) database information, execute organization tasks, (for example, shutdown) on the database, recoup the substance of a given document, and, at times, issue commands to the working framework.

Cross-site scripting (XSS) attack

XSS attacks utilize outsider web assets to run contents in the unfortunate casualty's internet browser or scriptable application. In particular, the attacker infuses a payload with noxious JavaScript into a website's database. At the point when the unfortunate casualty demands a page from the website, the website transmits the page, with the attacker's payload as a feature of the HTML body, to the injured individual's program, which executes the vindictive content. For instance, it may send the injured individual's treat to the attacker's server, and the attacker can separate it and use it for session seizing. The most hazardous results happen when XSS is utilized to abuse extra vulnerabilities. These vulnerabilities can empower an attacker to take treats, yet in addition log key strokes, catch screen captures, find and gather arrange data, and remotely access and control the unfortunate casualty's machine.

Birthday attack

Birthday attacks are made against hash calculations that are utilized to check the uprightness of a message, software or computerized signature. A message handled by a hash capacity creates a message digest (MD) of fixed length, autonomous of the length of the info message; this MD exceptionally portrays the message. The birthday attack alludes to the likelihood of discovering two random messages that produce a similar MD when prepared by a hash work. In the event that an attacker figures same MD for his message as the user has, he can securely supplant the user's message with his, and the recipient won't most likely identify the substitution regardless of whether he analyzes MDs. [7]

Phishing and spear phishing attacks

Phishing attack is the act of sending messages that give off an impression of being from confided in sources with the objective of increasing individual data or affecting users to accomplish something. It joins social designing and specialized slyness. It could include a connection to an email that heaps malware onto your PC. It could likewise be a connection to an ill-conceived website that can fool you into downloading malware or handing over your own data. [8]

Spear phishing is a very focused on kind of phishing movement. Attackers set aside the effort to direct investigation into targets and make messages that are close to home and applicable. Along these lines, spear phishing can be extremely difficult to distinguish and considerably harder to safeguard against.[8]

IV. CONCLUSION

Authentication is procedure of giving a user access to a data framework. There are three principle kinds of authentication instruments – password passage, savvy card, and biometric. Every authentication instrument works contrastingly and has their qualities and shortcoming. In this paper we audit various sorts of authentication instruments, their vulnerabilities, and suggest novel arrangements.

REFERENCES

[1] L. Dostalek J. Ledvina "Strong Authentication for Mobile Application" International Conference of Applied Elecronics č. IEEE CFP1569A-PRT pp. 23-26 September 2015.

[2] Q. Jiang J. Ma G. Li L. Yang "Robust Two-Factor Authentication and Key Agreement Preserving User Privacy" IJ Network Security vol. 16 no. 4 pp. 321-332 2014.

[3] Wang, X.M., Zhang, W.F., Zhang, J.S., Khan, M.K.: Cryptanalysis and improve-ment on two efficient remote user authentications scheme using smart cards. Computer Standards and Interfaces 29(5), 507–512 (2007)

[4] Li, C.T., Hwang, M.S.: An efficient biometric based remote user authentication scheme using smart cards.

Journal of Network and Computer Applications 33(1),(5) (January 2010)

[5] Hsu, C.L.: Security of Chien et al's remote user authentication scheme using smart cards. Computer Standard and Interfaces 26(3), 167–169 (2004)

[6] Sun, D.-Z., et al.: Weakness and improvement on wang-Li-Tie's user friendly remote authentication scheme. Applied Mathematics and Computation 170, 1185–1193 (2005)

[7] M. Farik, "Algorithm to Ensure and enforce Brutce force attack resilient password in routers," Algorithm to Ensure and enforce Brutce force attack resilient password in routers, vol. 4, no. 10, p. 5, 2015.

[8] Nadarajah Asokan Valtteri Niemi Kaisa Nyberg "Man-in-the-middle in tunnelled authentication protocols" Security Protocols. Springer Berlin Heidelberg pp. 28-41 2005..